TESTIMONY OF RICK ROWE, CEO, SAFEVIEW, INC.

"Leveraging Technology to Improve Aviation Security"

House Committee on Homeland Security,
Subcommittee on Economic Security,
Infrastructure Protection, and Cybersecurity

Wednesday, July 13, 2005

Testimony of Mr. Rick Rowe, CEO of SafeView, Inc.

Chairman Lungren, Ranking Member Sanchez, and other Members of the Subcommittee, I thank you for the invitation to testify before your Subcommittee today. My name is Rick Rowe, and I am the CEO of SafeView, Inc., a company that makes highly sophisticated security screening portals for checkpoints. I also serve our country as a member of the National Academy of Science's Committee on Assessing Technology for Transportation Security, and I strongly recommend to you the work of our Committee and its subsequent reports, but I wish to clarify that I am here today in my capacity as SafeView's CEO, and that my testimony is my own and not in any way to be construed as a position of the National Academy of Science.

It is my privilege to be with you this afternoon to discuss security checkpoints, and the process changes that I believe are necessary to get more new technologies into the field to improve the safety, speed, and effectiveness of these checkpoints. These changes apply for any venue, be it airport, rail or subway, government or private building, nuclear power plant, prison, or military checkpoint. All checkpoints for screening people have a great deal of commonality. All have threats or contraband they are trying to control, and entry or exit that needs to be efficient. All have a rush hour—meaning, peak throughput requirements—and all have a need to be safe for use around human beings.

I and members of my company have spent much of the last two years sitting at the most dangerous checkpoints in the world, principally in Israel's Gaza strip and of late, in Iraq, working on these very issues. Safety, efficiency, and throughput are the driving needs at checkpoints.

I truly believe that our nation does not deploy new solutions to address ever changing security threats and therefore improve our "checkpoints" as rapidly as it should or is able. This is critical not only to save lives, but to provide peace of mind that people are as safe as reasonably possible from tragic events such as those that just occurred in London. While not all attacks can be prevented, we can harden our targets and reduce our vulnerability. By hardening our targets, I mean making it obvious to all that this is a "hard checkpoint" to get through with hidden items. The technology and methods used need to create a very high probability that you will be caught. Terrorists and criminals do not like to try and get through "hard targets" and they know which ones they are. We all know that new technologies are needed to replace those of the 1970's such as metal detectors, which is still our backbone of technological capability.

As a small start-up with unique technology, we purposefully planned our testing and deployment of our technology in other countries first, because we knew that the United States government is extremely slow systemically in its implementation of new approaches.

We are not alone. Many start-ups, often holders of the most sophisticated and advanced technologies, do this as a matter of course. We all tend to "prove our solutions" elsewhere, if for no reason than investor pressure for quick results. We do not have the luxury of years of endless lab testing driving toward some perfect engineering solution that all too often works in the lab, but not in the field, or, at worst, provides diminishing returns when compared to lost time to market. For example, in the years a developing technology sat in the lab going from say, 80%

effective to 95%, or whatever criteria set, we lost all that opportunity to have at least a more effective solution than present methods, confuse our adversaries as they see targets harden, and learn what is important in the field, where it matters, to drive to higher levels of efficiency. In our view, there is no silver bullet. There is no single technology that makes us completely safe. Our view is to reap the benefits of developing solutions as they are perfected in the field, and layer them into an overall integration of systems that creates synergy so that the sum of the parts is greater than the whole.

In our particular case, we screen people for threats using millimeter waves. This is a totally safe technology, not ionizing radiation that frightens many, and one that was developed at the Pacific Northwest National Lab in the late 90's. It bounced around government labs for almost five years. But in just two short years, as a private company, we designed a commercial product, and, rather than wait for the United States to go through its motions, we actually spent the majority of our time in Europe, Israel, and other Middle Eastern locations, perfecting our design, because we knew we could quickly get into the field there. While we have worked with various U.S. agencies in parallel, we have, again, spent the bulk of our time with foreign governments, who are much more prone to encourage our use of what we call "beta" field testing. Some call it demonstration projects or pilot projects. What it all boils down to is that we take systems that may be early in their maturity and not be perfect solutions in the lab, but we get them out of the lab and into the field. Then we can adjust and tailor them to the threat and throughput requirements. It was because these countries were willing to put new technology in the field that allowed us and them to learn while strengthening on-going security.

There are successes in the military side. Shortly after the terrible bombing that killed our troops in Mosul, Iraq, last December, there was a rush as the U.S. military reached out to industry to look at technologies to protect U.S. troops from IED's and, in our case, walk-in suicide bombers. To the eternal credit of key members of our military, I was able to convince them to let us, at only a transportation charge to the government, set up our systems to prove their worth in Iraq.

Today we have two systems in Iraq at checkpoints that are exceeding anyone's expectations, even mine. They have totally replaced hand pat down searches, which was the only previously used method of checking for everything from suicide bombers to normal contraband. It has been proven to be safer, faster, and more effective.

I have spent well over 120 hours in the past two months, sitting side by side with our soldiers in Iraq. Observing, coaching, learning………and changing our technology design to meet their needs. I leave again this Sunday to sit at the checkpoints with them again. Not a five minute visit for an overview, but rather days to understand their needs and missions. This is because we are committed to helping protect them by providing the best technology possible. I think most of the companies here today, if given the opportunity, feel the same way.

As an important aside, it is also critical to understand that hardening of checkpoints is as much about deterrence as catching someone. I often get asked about "how many explosives have you discovered in Iraq or Israel." This misses the point entirely. The worst checkpoint in the world for suicide bombers in 2004 was in Israel. They screened over 1.5 million people, yet had only 2 suicide bombers and two outright attackers. But these four incidents resulted in over 19 soldiers

killed and scores injured. Some who were maimed forever. But everyone now knows this checkpoint is being hardened and the Concept of Operation changed. By Concept of Operation, I mean the method of how you run the checkpoint. It is the process or way of screening people, the melding of technology and people who operate the system.

One of the biggest changes in systems today is that so much is software based. You can get the physical hardware into the field and keep improving and updating the software as you go. Enjoy the advantage of having faster time to market, knowing the system can keep getting better. We recently did this in Iraq. After sitting with the soldiers working the Concept of Operation at the checkpoint, we together decided they needed more "views" of the people being screened. I called back to the U.S. on my cell phone and our engineers emailed me a new software program, and within 24 hours I had that update installed and operating.

This coupling of getting into the field early and working together on the Concept of Operation is where you learn what works and what does not. You learn and adapt both the Concept of Operation and the technology. What needs to be changed in each and what does not. You do not learn this in the lab.

This doesn't mean the agencies and labs don't have a critical mission. They do. In my opinion they should concentrate on initial testing and review on an expedited basis to ensure they technology does indeed have promise and does have the potential to reach some threshold of efficiency, but let it be practical with room to improve. Don't require perfection right out of the blocks. Prove that it is safe to use with and around people. We need our government agencies to be at the threshold, positively encouraging and helping industry provide the answers, not some onerous gatekeeper that refuses to let anything pass without enormous scrutiny and over-engineering that serves no real purpose. Tell us in industry what the problem is, not the solution. We in industry are and need to be treated, as suppliers and solution partners, not as adversaries who cannot be trusted.

What this country needs now, in our airports, in our subway and train stations, and in our buildings is more "pilots" or "beta-testing." If we wait for our agencies and their labs to churn out the perfect solution…..the silver bullet…..we will have a very long wait…..if it comes at all. In my past life in commercial and industrial businesses, we used to have a favorite expression….it is time now to end the engineering and deliver the product. It is time now for our Nation to adopt the same approach. We need rapid movement of technologies from the lab to the field.

And please don't pick a single technology…..Don't narrow your choices too soon…let good companies prove their mettle and get their technology out of the lab and into the field. We will all learn and grow from it and the best solutions will surely rise to the top and be the commercial successes companies hope for, and our Nation, its citizens, and our men and women in uniform will be safer.

About SafeView

SafeView, Inc. is a privately held developer of systems using patented detection technology for various security applications, and is based in Santa Clara, CA. SafeView holds an exclusive license to commercialize the active millimeter wave holographic technology from Battelle,

which manages the Pacific Northwest National Laboratory for the Department of Energy. SafeView's system uses an active millimeter wave technology that is safe and offers unique detection of objects made of metal, plastic, ceramic, and other materials that may be hidden under clothing without using ionizing radiation. SafeView's system offers a more effective and less intrusive alternative to metal detectors, pat down searches, and other means used to ensure safety in public areas. Additional information about SafeView can be accessed from the company's website at http://www.safeviewinc.com.